

throughout the state. As digital evidence becomes increasingly prevalent in police work, some agencies are training their own staff to handle this type of evidence. Absent that local resource, agencies can submit digital evidence for examination to the ICAC office or the Kentucky Regional Computer Forensic Laboratory in Louisville.

Digital evidence comes in a wide variety of types and sizes. Complexity and capacity determine the amount of time required to process evidence.

“What has changed the most over the years is the sheer size of the media we deal with,” said Detective Chris Frazier, a forensic examiner with the KSP Electronic Crime Branch. “When I started working at the Electronic Crime Branch, a 50-gigabyte hard drive was huge. Now it’s not unusual to find one terabyte drives during exam requests. Another significant change involves the rapid advancement in cell phone technology. Cell phones are becoming more and more like mini computers.”

In 2011, the KSP Electronic Crime Branch digital forensic lab examined roughly 29 terabytes of data. To try and put that into perspective, just one megabyte of data is about 1,000 sheets of paper with each page completely filled front and back. Considering that, if information from the 29 terabytes examined last year alone were printed front and back, that paper stacked would be more than 900 miles high. That’s roughly the distance from Chicago to New Orleans or the distance from the ground beyond our atmosphere into outer space.

There are several misconceptions about child pornography. Some believe child pornography refers to photographs or videos of babies in the bathtub. Others think of teenagers in pigtails and schoolgirl uniforms. The child pornography faced by ICAC Task Force officers is far darker and more grotesque than many could imagine. It involves pictures and videos of young children, often in diapers, being violently molested. During a National Juvenile Online Victimization Study in 2005, it was discovered that more than 80 percent of the people arrested for child pornography had saved images of prepubescent children, and 80 percent had images of minors being sexually penetrated. As far as age, 83 percent had images of children between the ages of six and twelve years. Not only do these children bear suffering and brutal

trauma of sexual victimization, they continue to be exploited every time their images are traded online by individuals seeking sexual gratification.

As technology grows, so does the opportunity for child pornographers to exploit it. Social networking sites, chat rooms, file-sharing programs, message boards and forums all now make it easier for people to trade child pornography and connect with children. While computers and cell phones remain the primary means of communication, gaming systems that can connect to the Internet give predators yet another way to gain access to children electronically.

A decade ago, parents worried about the chat rooms their children visited on a

desktop computer. Today, it’s much easier to contact children now that everyone can have the Internet in their pocket.

Most parents have become more aware of the basics, such as keeping the computer in the family room, but more needs to be done. One goal of the task force is to promote community awareness and prevent victimization. Last year alone, Kentucky’s task force conducted 85 presentations in schools and at community groups – reaching nearly 6,000 people.

Technology is both a blessing and curse. It makes our daily lives easier, however, it can leave our children exposed to predators. We must teach our children to use technology wisely and be aware of the dangers lurking on the Internet. 

